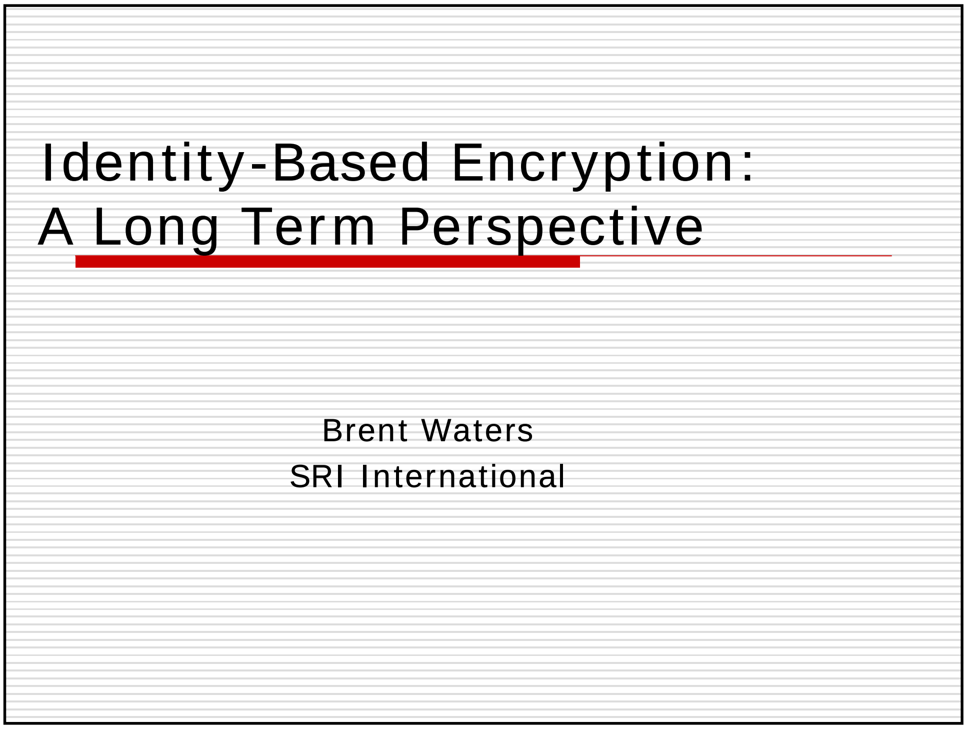
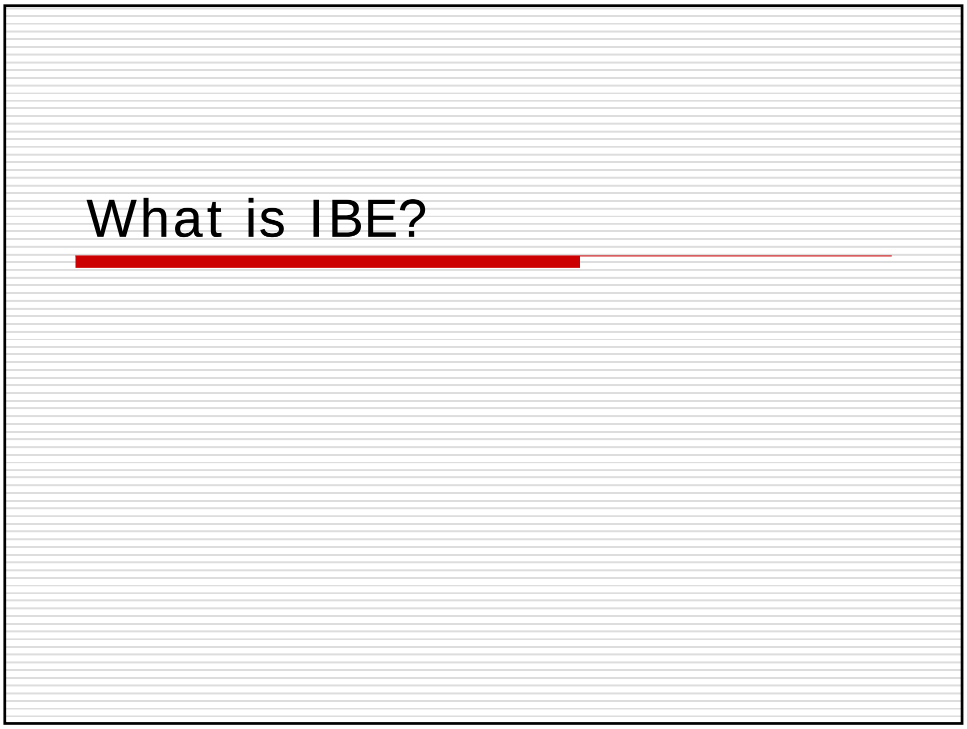


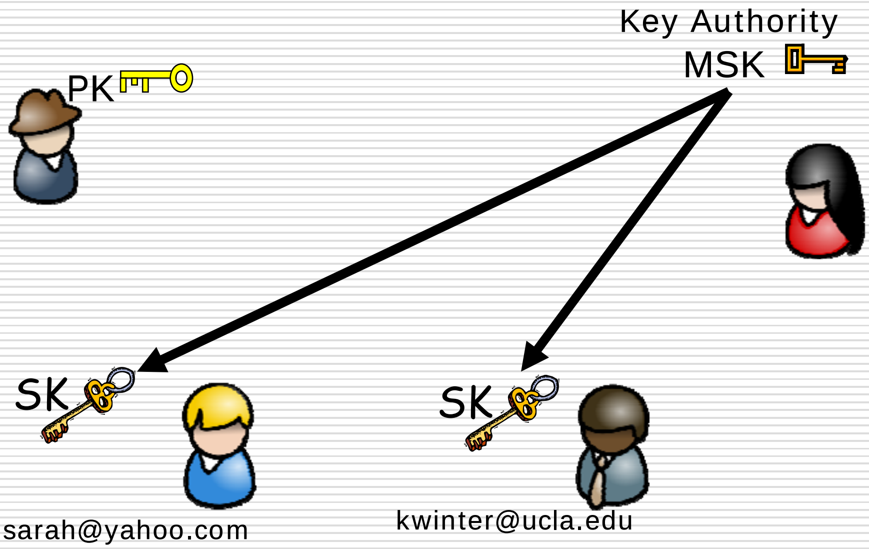
Identity-Based Encryption:
A Long Term Perspective

Brent Waters
SRI International



What is IBE?

Traditional View



Key Authority

MSK

PK

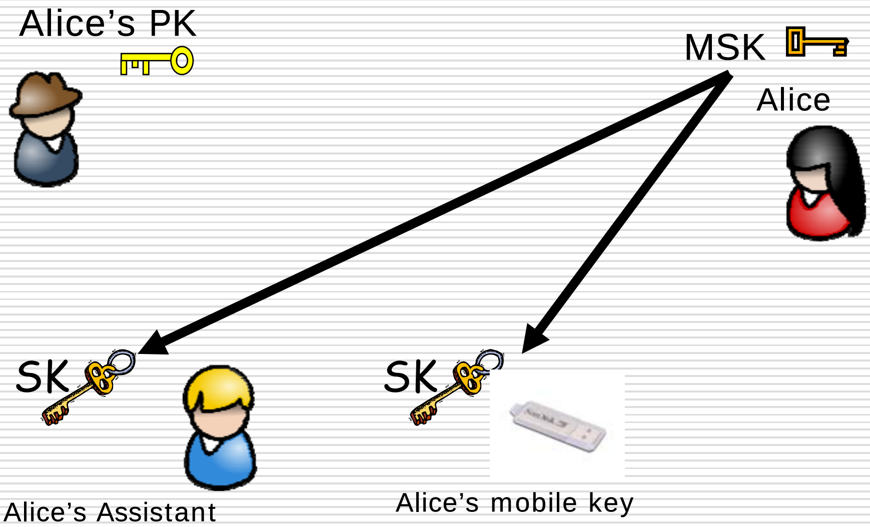
SK

SK

sarah@yahoo.com

kwinter@ucla.edu

Managing Your Own Data



Alice’s PK

MSK

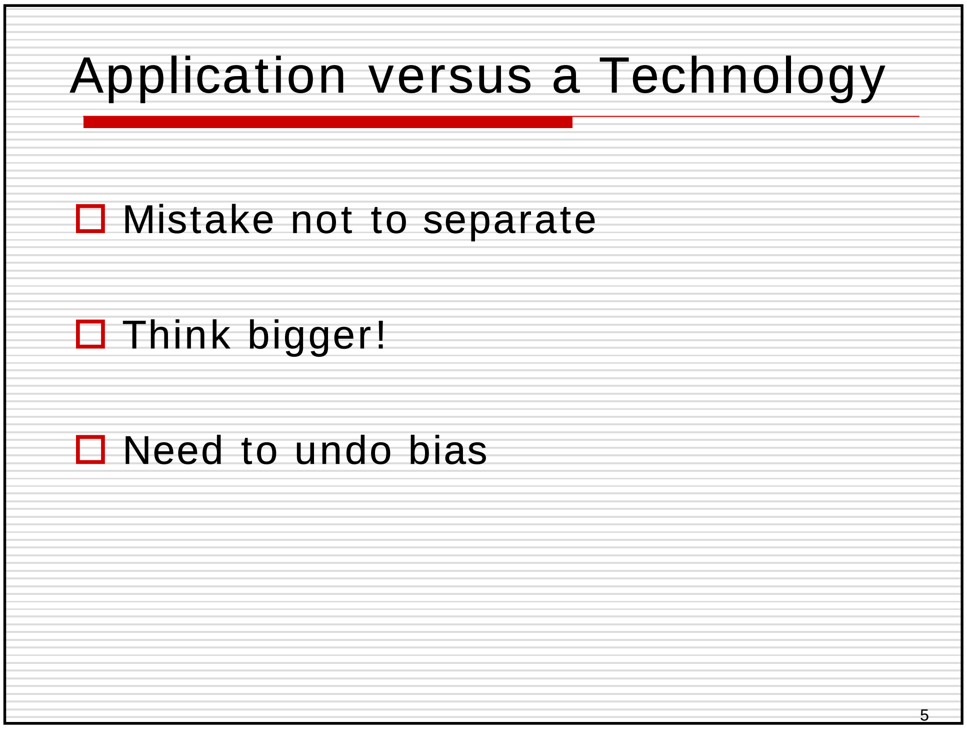
Alice

SK

SK

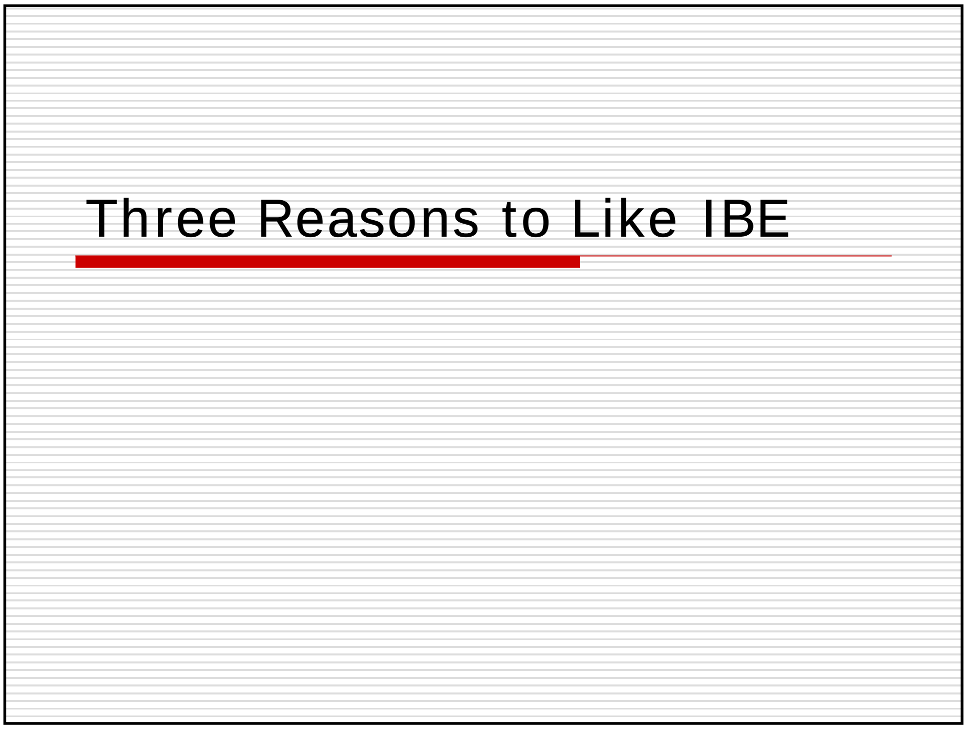
Alice’s Assistant

Alice’s mobile key

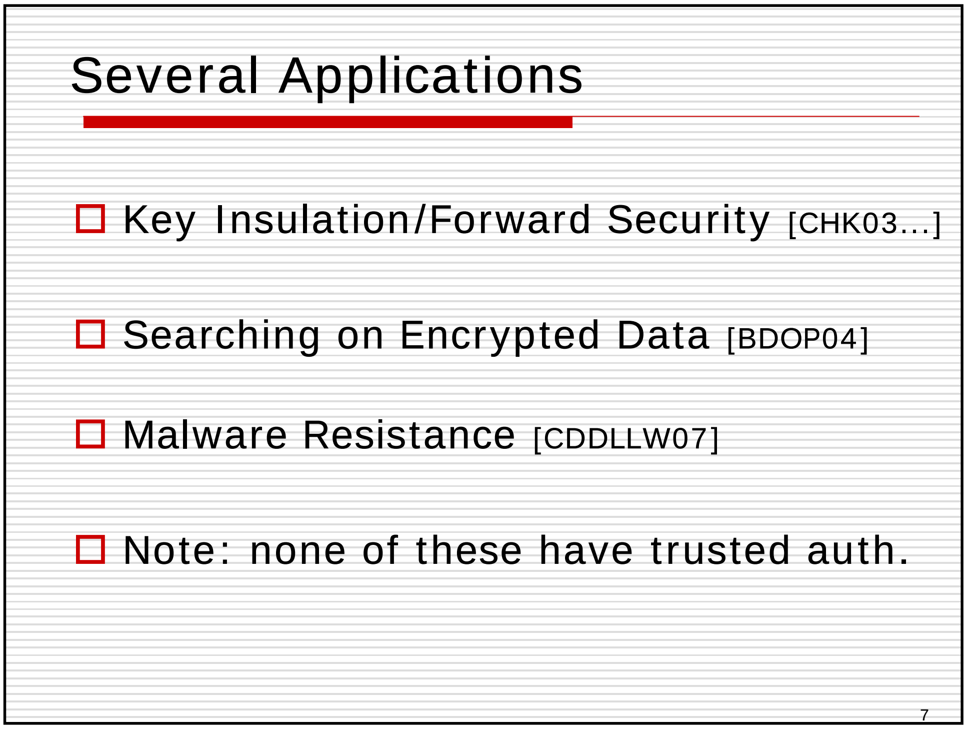


Application versus a Technology

- □ Mistake not to separate
- □ Think bigger!
- □ Need to undo bias

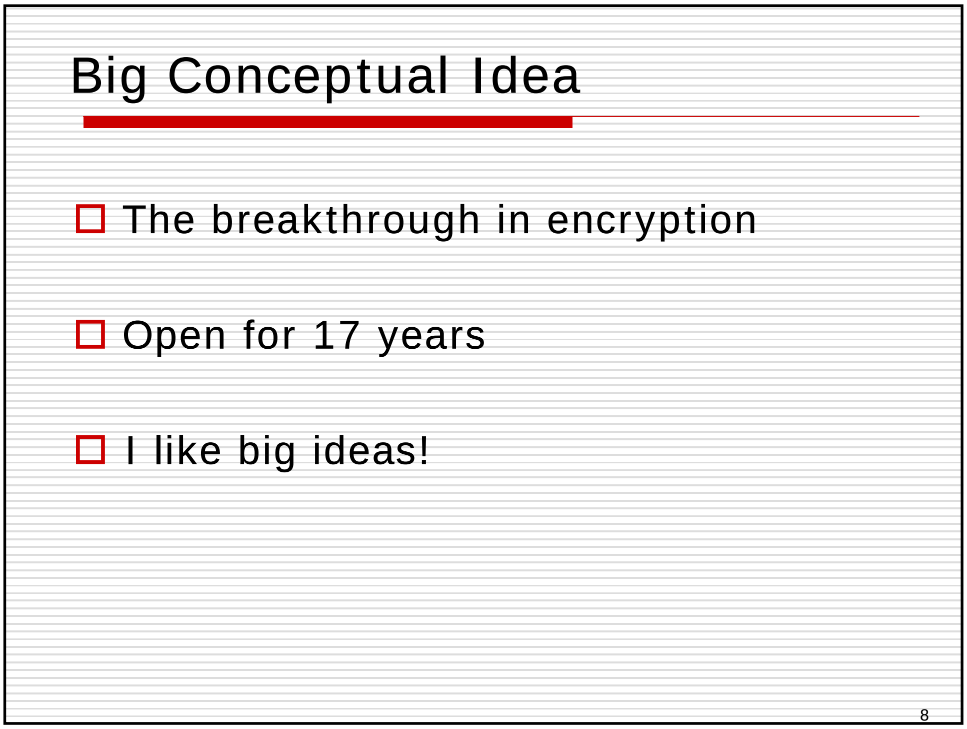


Three Reasons to Like IBE



Several Applications

- Key Insulation/Forward Security [CHK03…]
- Searching on Encrypted Data [BDOP04]
- Malware Resistance [CDDLLW07]
- Note: none of these have trusted auth.



Big Conceptual Idea

- The breakthrough in encryption
- Open for 17 years
- I like big ideas!

Thinking Back to Public Key Crypto

- Before: Do we really need it?
- Engineer around it?
- Now:
  - SSL
  - Software Patches

Thank you